KU LEUVEN
CENTRE FOR IT & IP LAW

imec

Encryption in the GDPR

How a technical requirement can transform trust

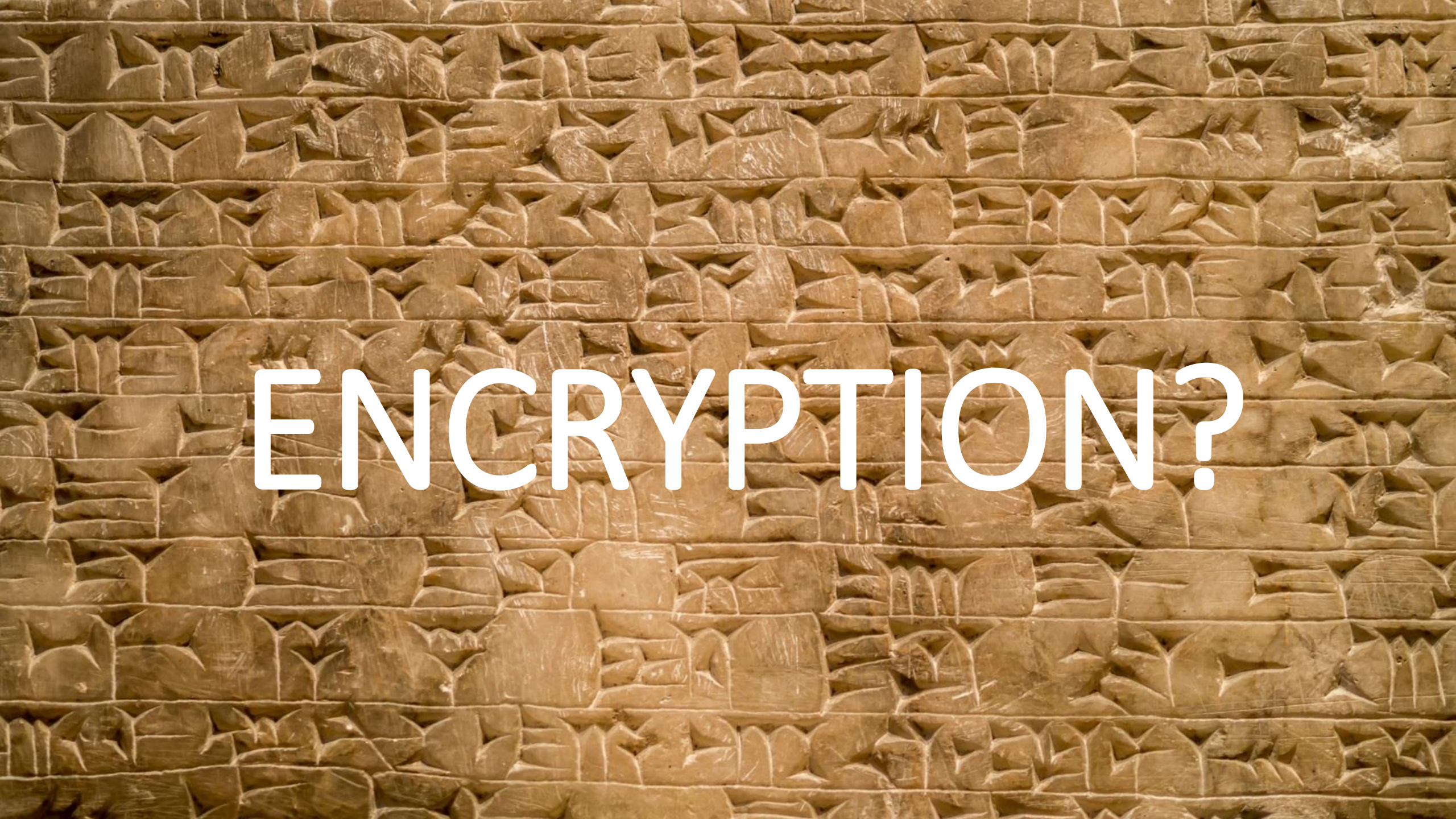
Griet Verhenneman
KU Leuven – CiTiP – imec
HEAT workshop
27/11/2017

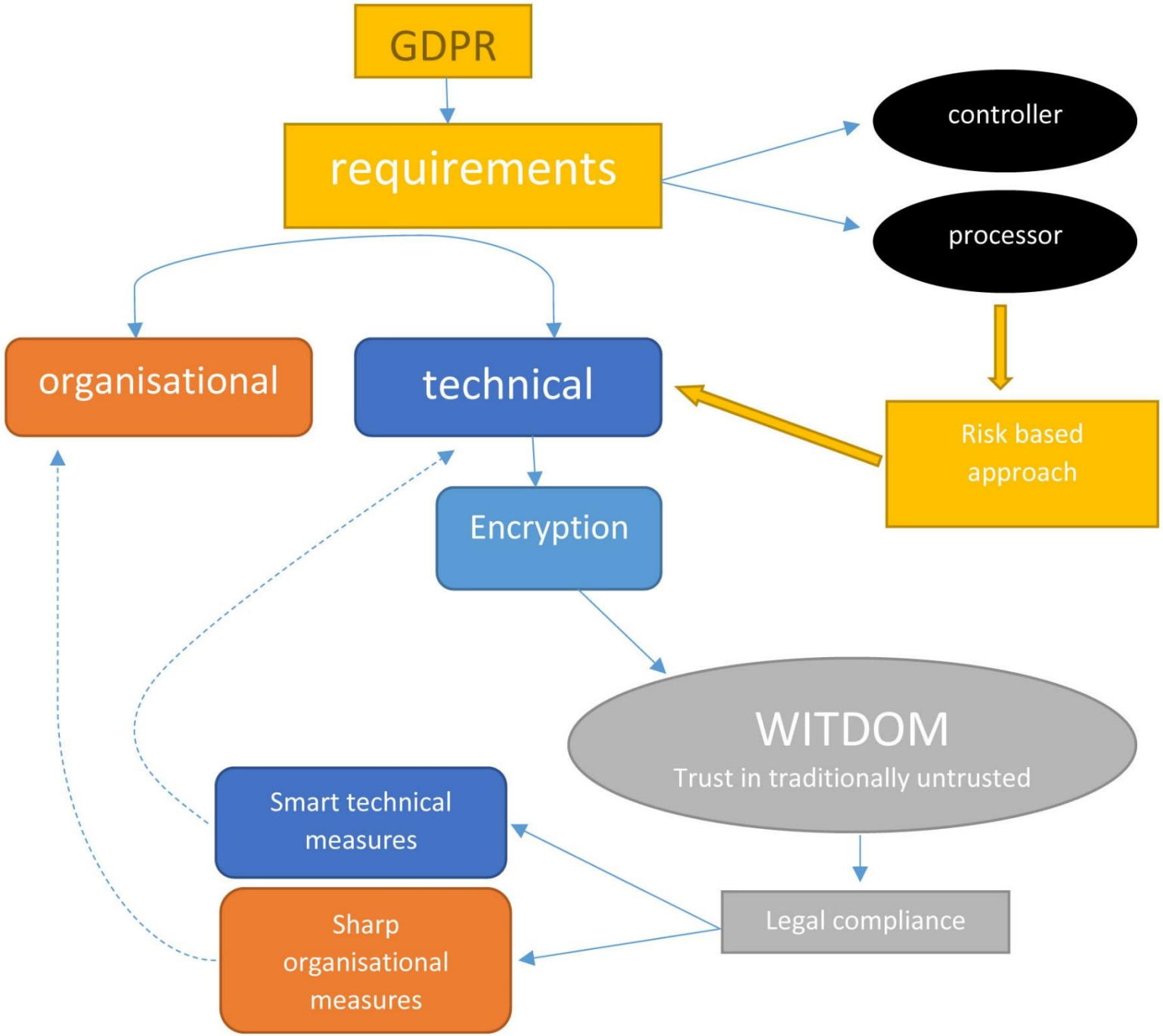
GDPR

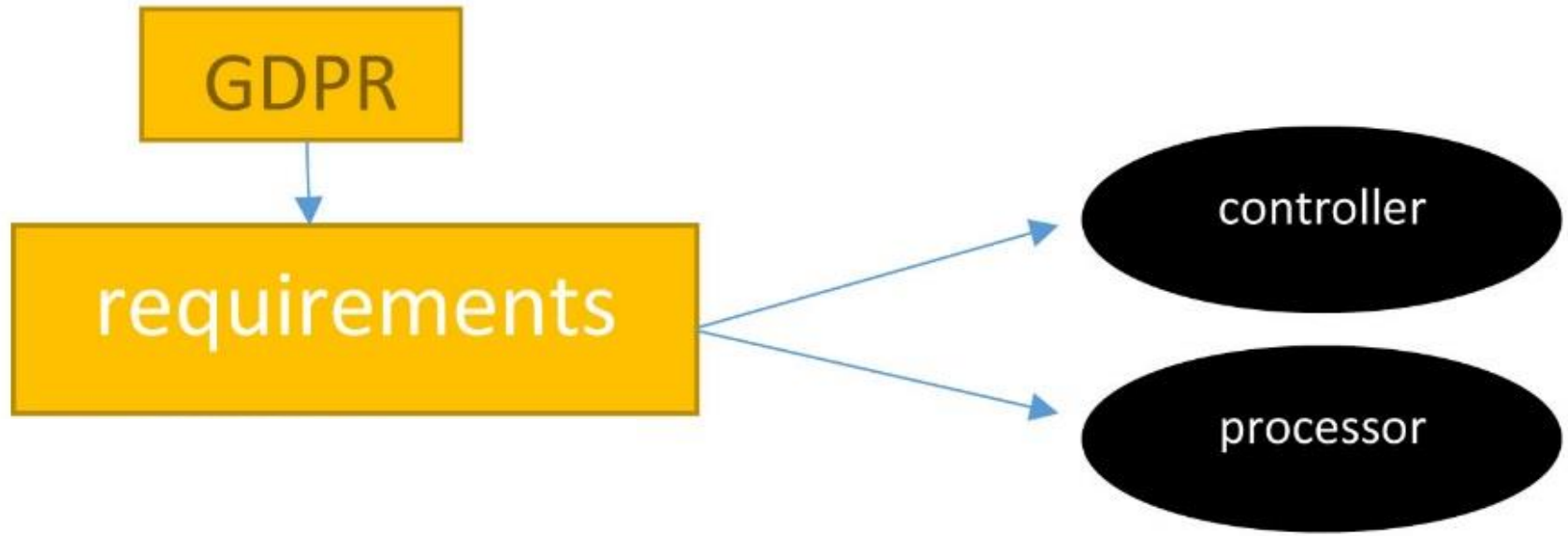
* basic protection mechanism

* for any operation

*performed on data relating to identifiable natural persons.


ENCRYPTION?


GDPR
requirements
controller
processor
organisational
technical
Risk based approach
Encryption
WITDOM
Trust in traditionally untrusted
Smart technical measures
Sharp organisational measures
Legal compliance


GDPR
requirements
controller
processor

GDPR roles: controller, processor

- Controller:

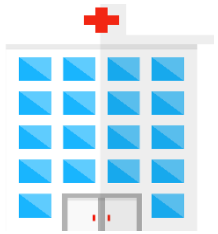
  Person, company or other body which **determines** the purposes and the means of the data processing.

- Processor:

  Person, company or other body which processes personal data **on behalf of** the controller.

- Other roles:
  - Recipient: person, company or body to which data are disclosed (e.g. processor or new controller)
  - Third party: person, company or body to whom data are transferred but who is external to the organisation of the controller and processor (e.g. new controller, researcher,…)
  - Data subject: natural person who's data have been processed

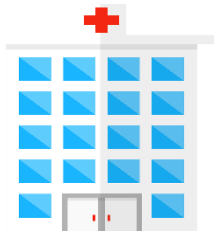
Example



Belgian Cancer Registry

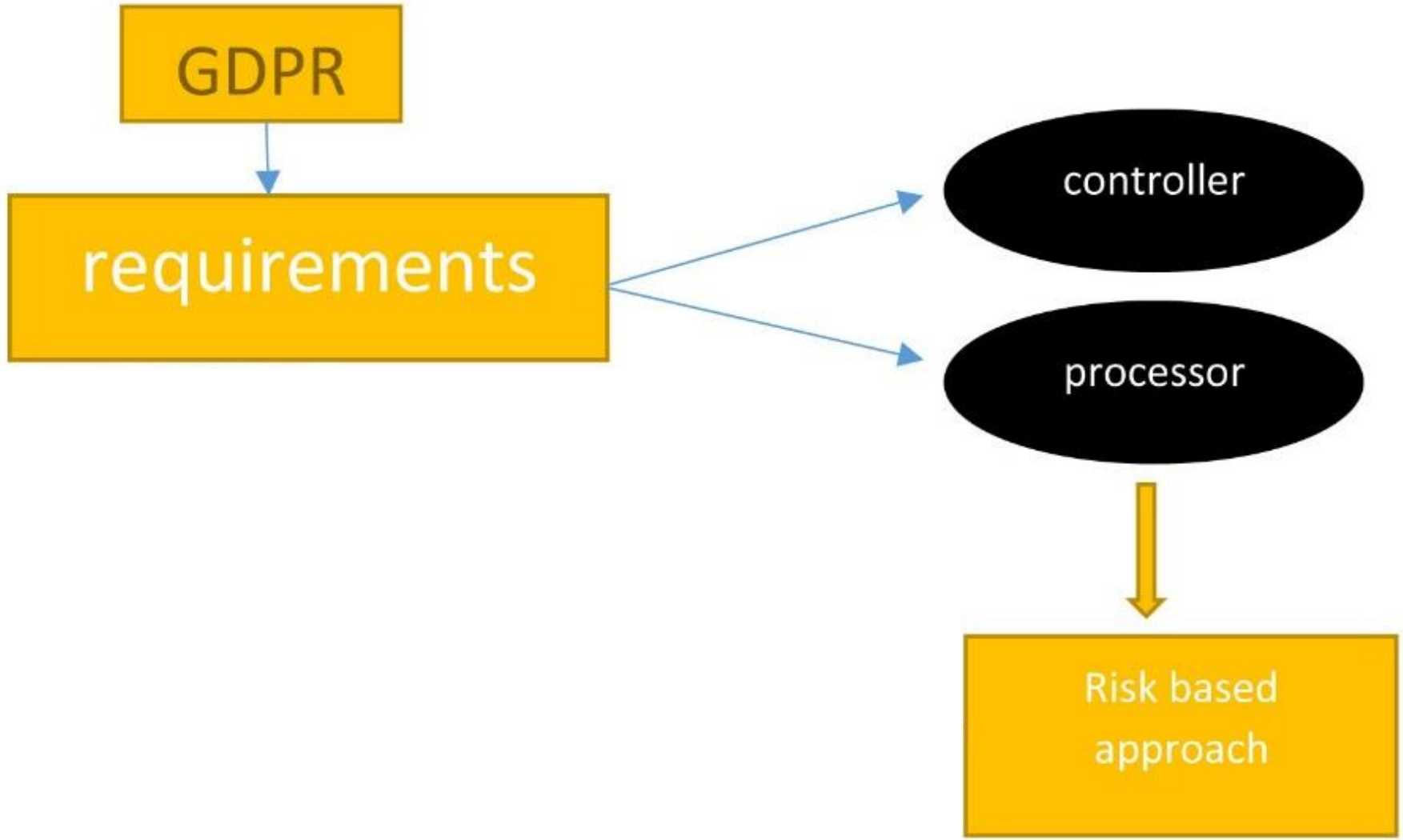
Example

processors



Belgian Cancer Registry

new controller


GDPR
requirements
controller
processor
Risk based
approach

Risk in GDPR

Recital 9: “The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or **a widespread public perception that there are significant risks to the protection of natural persons**, in particular with regard to online activity.”

- Awareness -> obligation to make people aware of the risks in data processing
- Special categories of data -> specific protection for high risk categories of data
- Security -> minimisation of the risks

Recital 76: “The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. **Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk**.”

Risk based approach

Before GDPR: system of notifications placed risk estimation at Data Protection Authority

GDPR: no notifications to DPA, but internal risk assessments

- Data Protection By Design
- Data Protection Impact Assessment
- Data Breach notifications to data subject

} all based on internal assessment of risks

= Responsibility of data controller and data processor:

EVALUATE and MITIGATE

Example: ENISA formula for severity of data breach (2013)

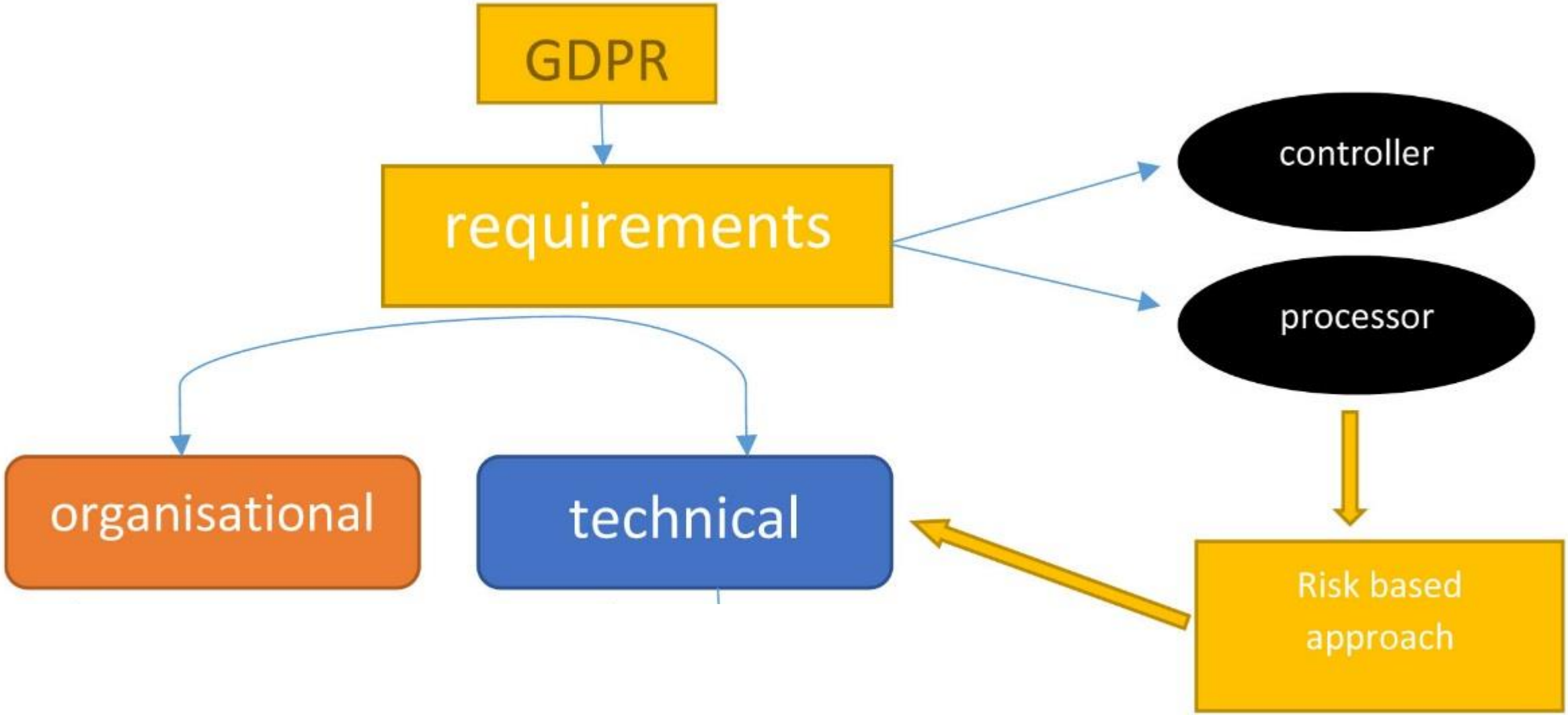
$$SE = DPC \times EI \times CB$$

Severity of the data breach =

data processing context x ease of identification x circumstances of the breach

Takes into account:

- Type of data that is being processed (simple, behavioural, financial, sensitive)
- The context of the data processing (quantity of data, vulnerable data subjects, use for profiling)
- How easy it is for a party to univocally match to a data subject (direct or indirect identification)
- Loss of security (confidentiality, integrity, availability) and malicious intend


GDPR
requirements
controller
processor
organisational
technical
Risk based approach

Long list of requirements to protect the data subject

#181			Third country data transfers	All third country data transfers, including onward transfers are subject to the conditions of Chapter V GDPR.	Mandatory	Organisational		YES – new provision
#181				The suitable safeguards for third country data transfers shall be assessed and documented by the controller or processor.	Mandatory	Organisational		YES – new provision
NEW (#181)			Third country data transfer + transparency	When personal data are transferred to a third country or an international organization the data subject needs to be informed of the appropriate safeguards related to the transfer.	Mandatory	Organisational		YES – new specification to the right to information
NEW			Security	DPIA: An assessment is made (and repeated on periodic intervals) to evaluate what measures should be taken to have an appropriate level of security. This assessment includes: the state of the art, the cost of implementation, the nature, scope, context and purposes of the processing, the risks of varying likelihood and severity of rights and freedoms of natural persons.	Mandatory OR Desirable	Organisational Multidisciplinary		YES – new explicit security requirement
#182				Pseudonymisation is applied as a security measure wherever possible.	Mandatory	Technical		YES – the explicit reference to pseudonymisation is new
#182				Encryption is applied as a security measure wherever possible and proportionate	Mandatory	Technical		YES – new explicit security requirement
#182				Ongoing confidentiality, integrity, availability and resilience of	Mandatory	Technical		YES – new explicit security requirement

Examples of requirements extracted from the WITDOM GDPR requirements classification

GDPR requirements

- Organisational requirements

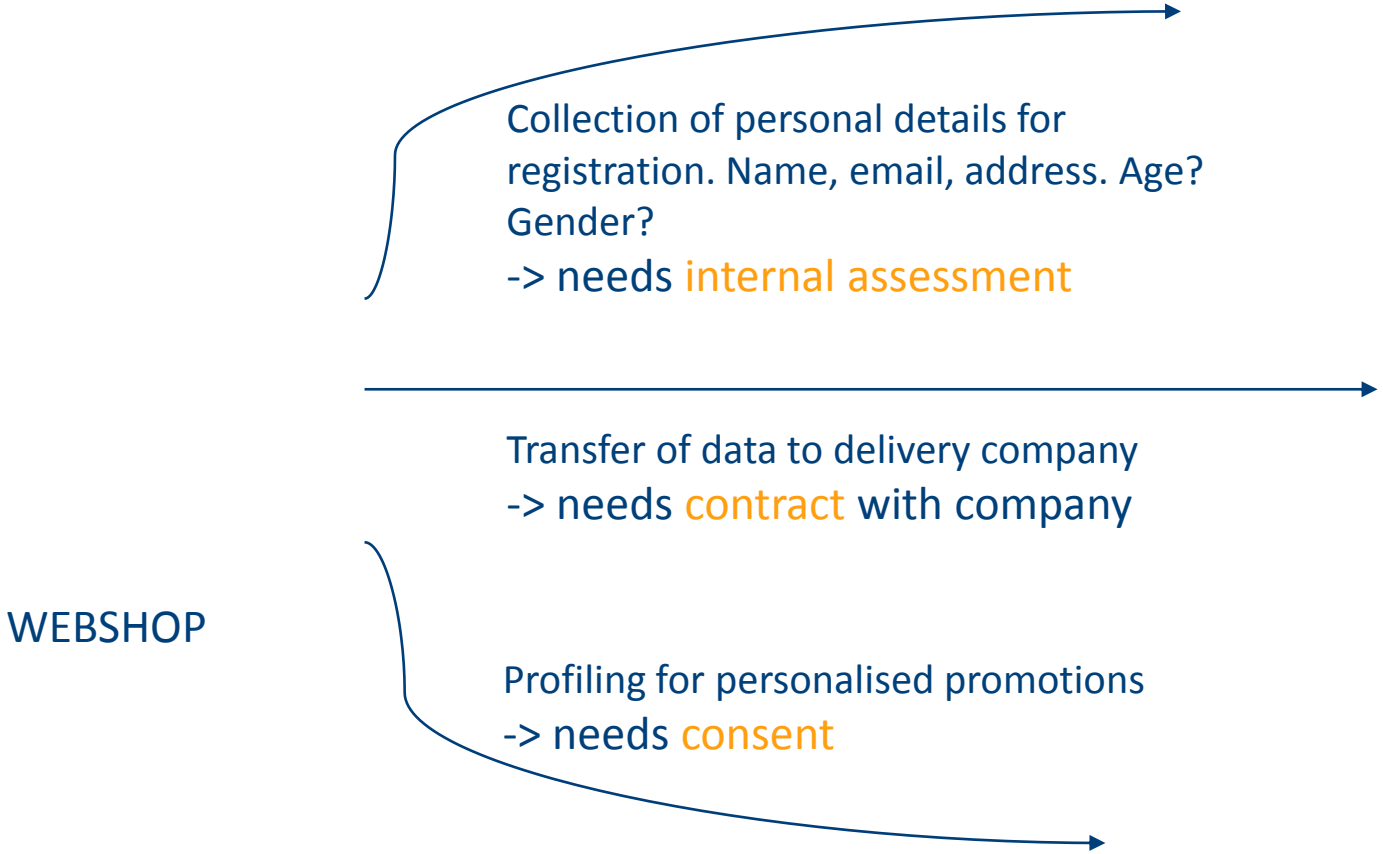
  Requirements which make you think about why and how you are going to process personal data, which data you need to do what you want to do (and which data you don't need) and for how long you need these data. But also requirements to organisational measures against loss, destruction or damage of data.

- Technical requirements

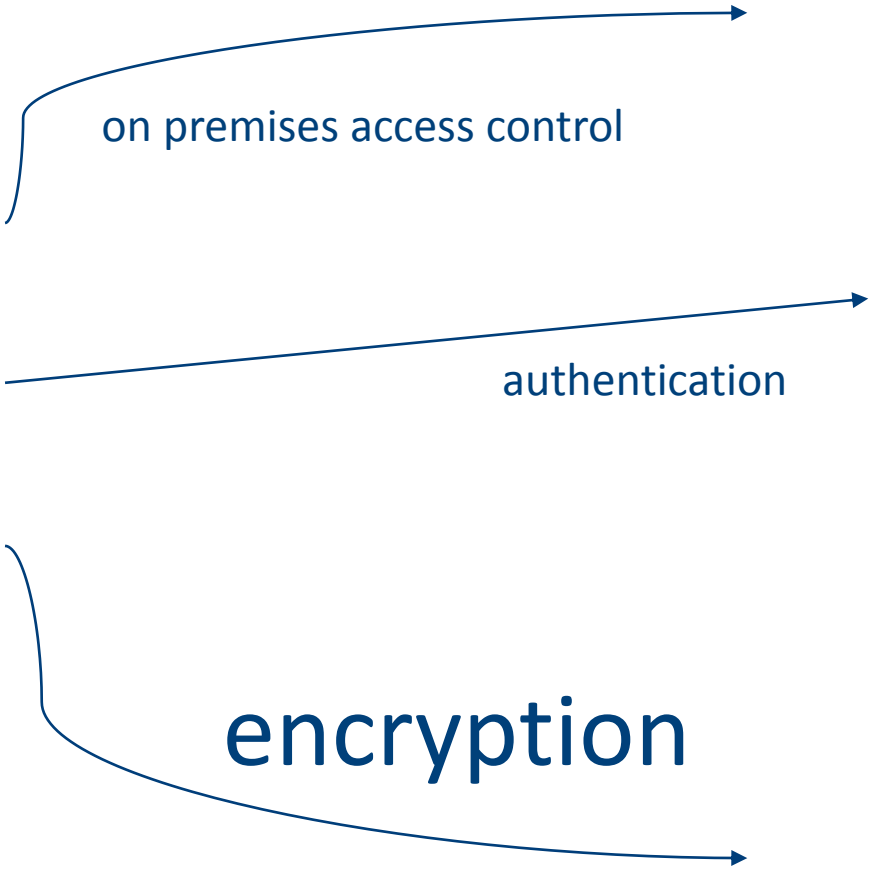
  Appropriate technical measures which ensure appropriate security of the personal data.

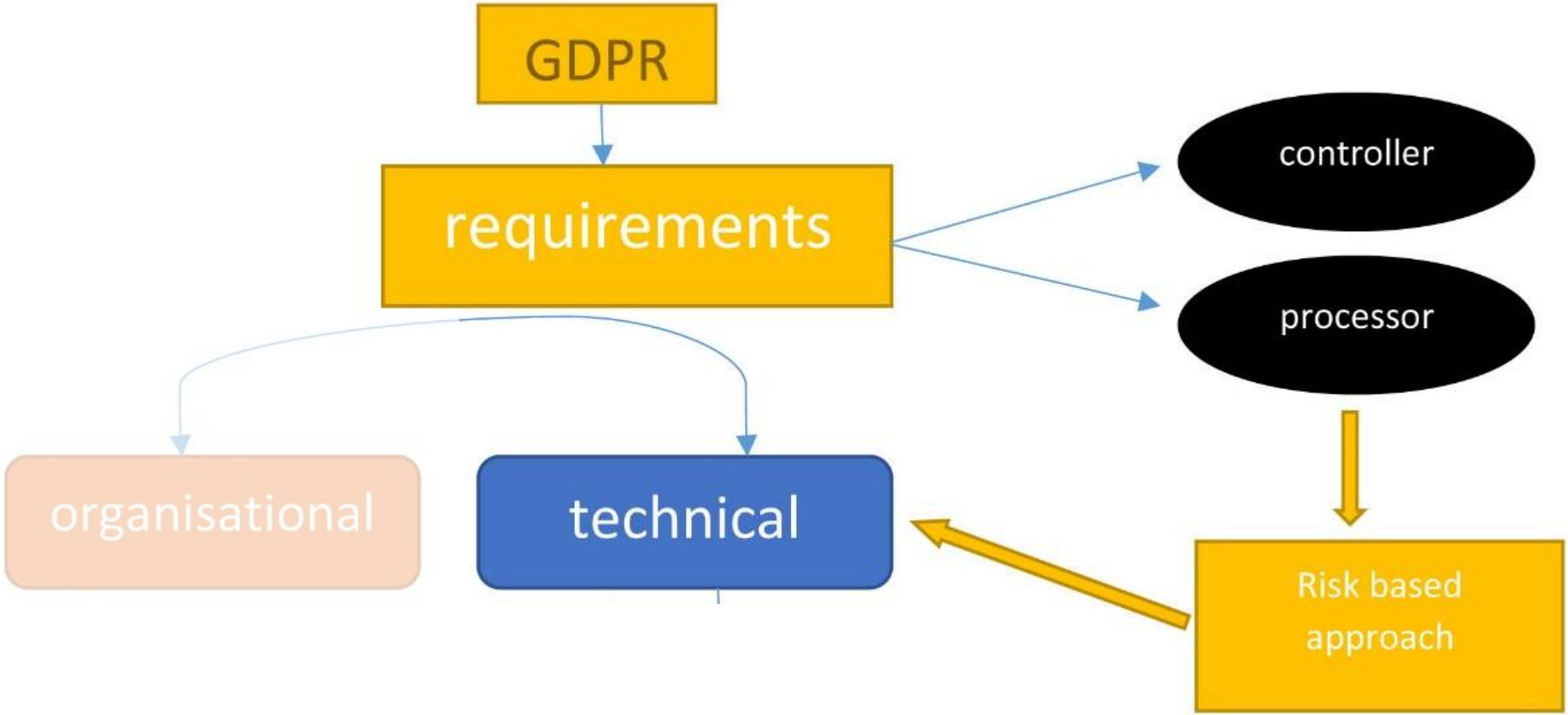
  And technical tools which can support obligations of the controller and the processor.

Example organisational measures



Example technical measures




GDPR
requirements
controller
processor
organisational
technical
Risk based approach

Technical requirements in GDPR

GDPR is technology neutral

- Applicable to all processing operations, no matter by which technology
  - Recital 15: "The protection of natural persons should be ***technology neutral*** and should ***not depend on the techniques used***."

  --> Prevent circumventions

- Agnostic in terms of technological measures which need to be implemented
  - Article 5, f) integrity and confidentiality: "personal data shall be processed in a manner that ensures ***appropriate*** security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using ***appropriate*** technical or organisational measures"
  - Article 32, 1.: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement ***appropriate*** technical and organisational measures to ensure a level of security appropriate to the risk"

Technical principles in GDPR

Technology neutral and agnostic to technical measures, but with attention for few principles:

- Pseudonymisation
- Integrity
- Availability
- Confidentiality

Pseudonymisation

- Article 25: "…the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation,…"

- Recital 28: "The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations."

- Recital 29: "In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should,…"

- Article 6, 4.: "… the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: […] the existence of appropriate safeguards, which may include […] pseudonymisation"

Integrity

- Article 5, (f): “personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures” (integrity and confidentiality)

- Recital 49: “The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security i.e. […] integrity of stored or transmitted personal data […] constitutes a legitimate interest of the data controller concerned.

- Article 32, 1. (b): “the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the ability to ensure the ongoing […] integrity […] of processing systems and services”

Availability

- Article 32, 1. (b): “the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including the […] availability and resilience of processing systems and services”

- Article 32, 1. (c): “the controller and the processor shall implement appropriate technical and organisational measures to ensure […] the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident”

Confidentiality

- Article 5, (f): “personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures” (integrity and confidentiality)

- Recital 39: “Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.”

- Recital 49: “The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security i.e. […] confidentiality of stored or transmitted personal data […] constitutes a legitimate interest of the data controller concerned.”

- AND… Recital 83: “In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, **such as encryption**. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected.”

Encryption in GDPR = valuable safeguard

- Compatible use
  - Article 6, 4.: "… the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: […] the existence of appropriate safeguards, which may include encryption or pseudonymisation"
- Security measures
  - Article 32, 1. (a): "[…] the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate the pseudonymisation and encryption of personal data"
- Data breach notifications
  - Article 34, 3. (a): "The communication to the data subject shall not be required if any of the following conditions are met: the controller has implemented appropriate technical and organisational protection measures, […], in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption"

Anonymised data are out of scope

But be aware:

- anonymisation in GDPR is always one way!
- ≠ pseudonymisation or coding
- ≠ encryption

Anonymisation in GDPR

Recital 26: “The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.”

Criteria to be identifiable:

- Individual can be singled out
- By controller OR any other person
- Taking into account all means reasonably likely to be used
  - Cost and amount of time required
  - Available technology at time of the processing
  - Technological developments

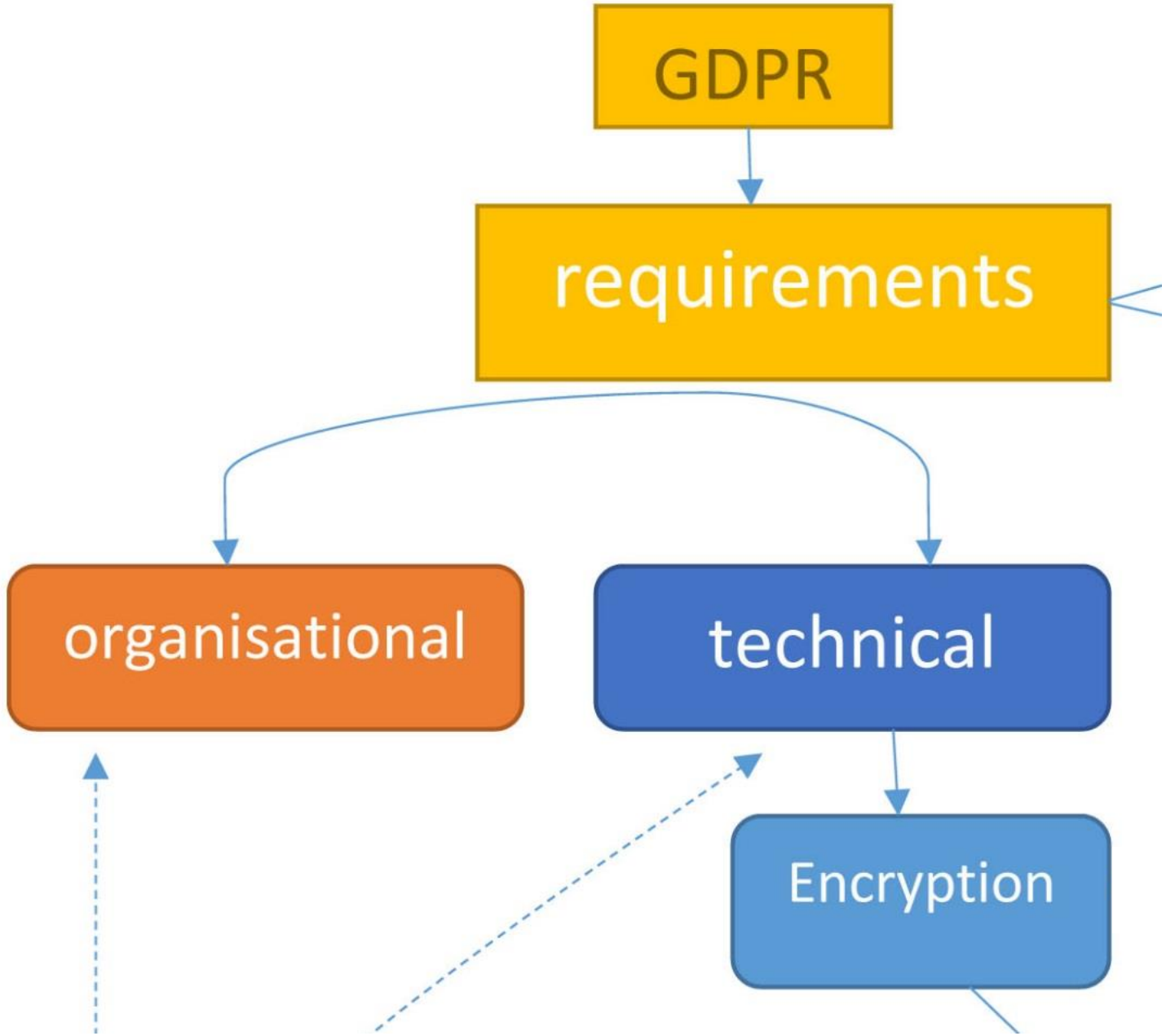
Anonymisation in GDPR

Criteria render the concept in many contexts to an illusion

- Article 29 WP (2014): “it is critical to understand that when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data.”

But next thereto, in many situations also redundant.

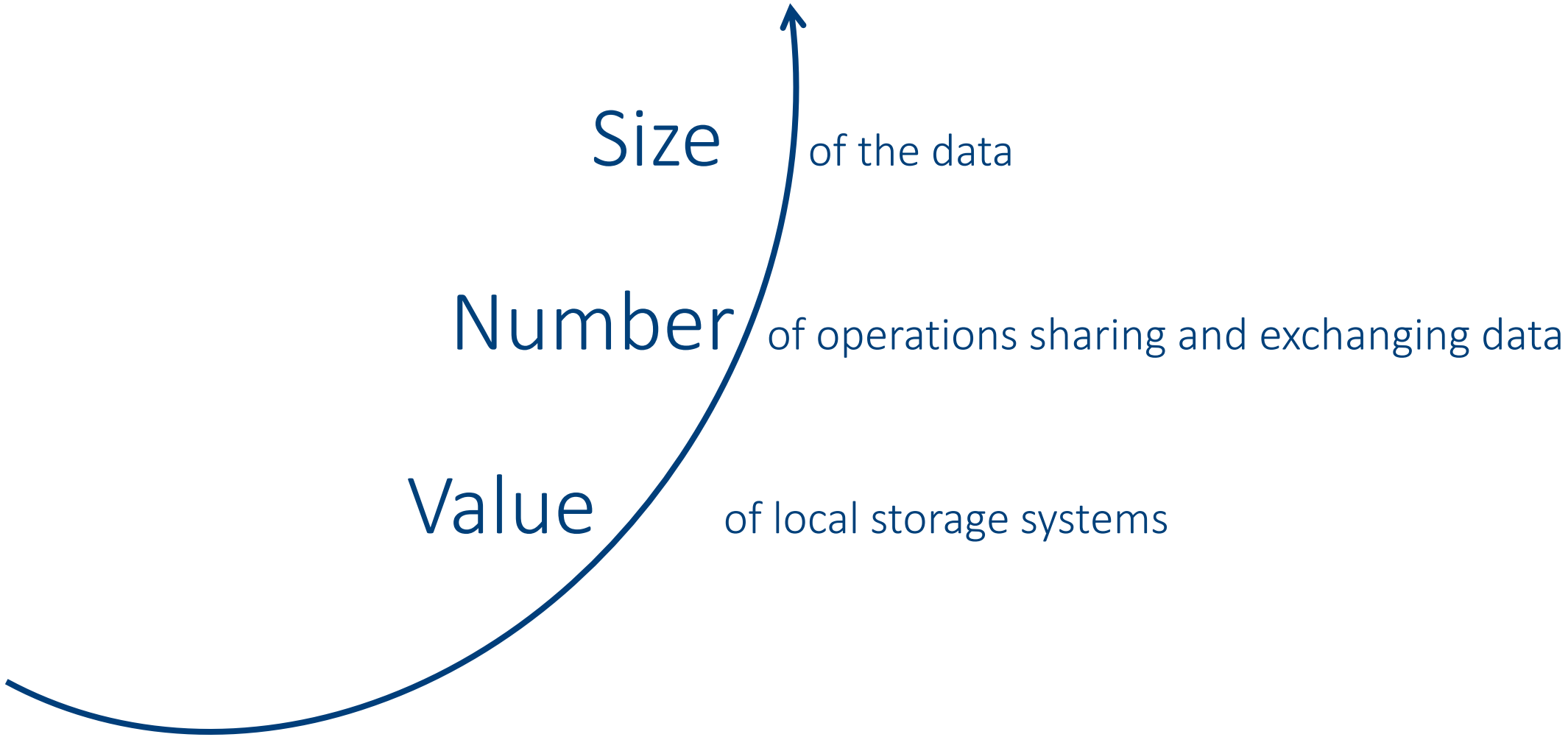
- Natural preference for pseudonymised data e.g. in research.


GDPR
requirements
organisational
technical
Encryption

Why encryption?

Recital 9: The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or **a widespread public perception that there are significant risks to the protection of natural persons**, in particular with regard to online activity."

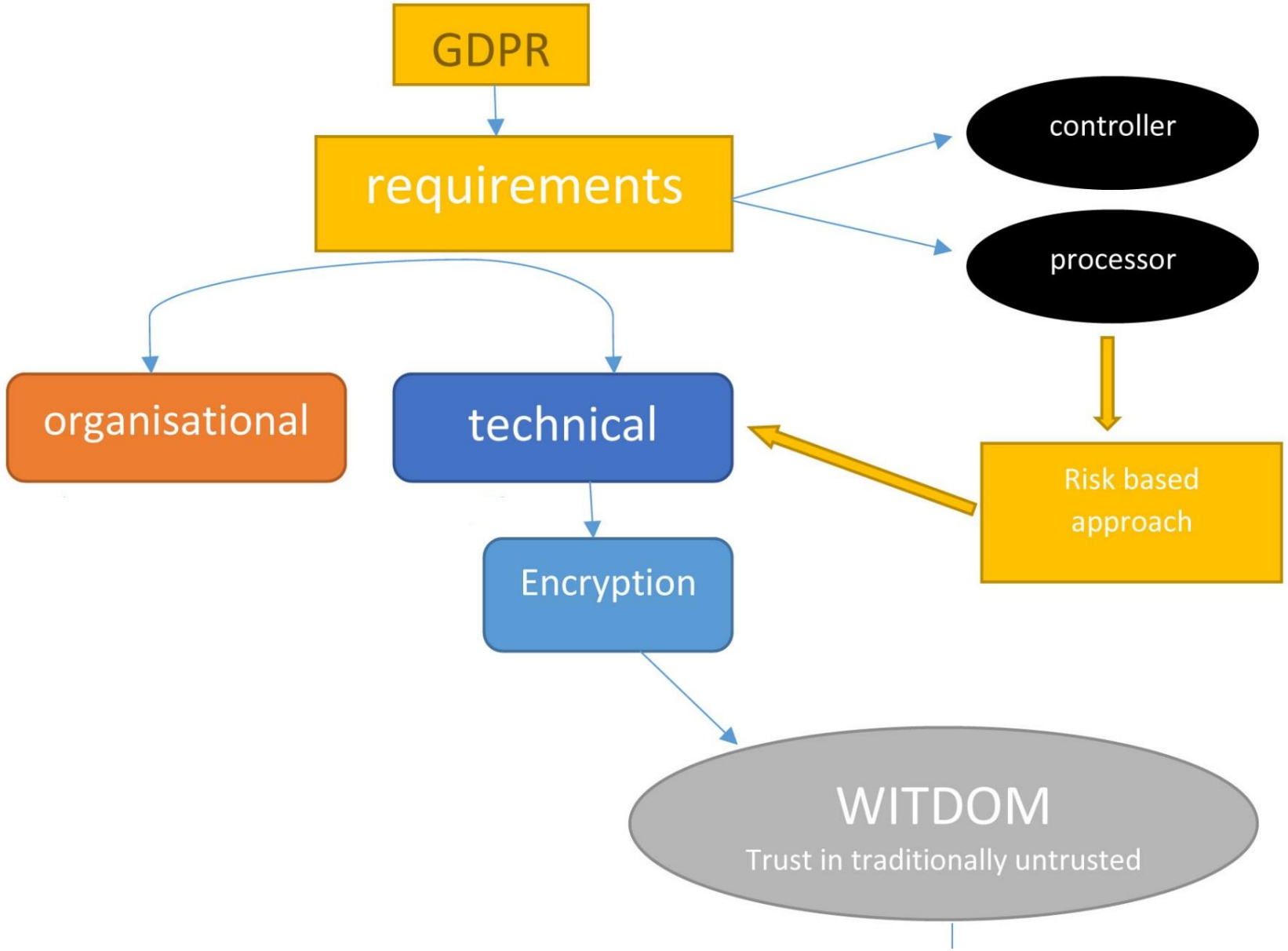
--> Directly related to off-site storage and computation


Size
of the data
Number
of operations sharing and exchanging data
Value
of local storage systems

Control?
Transparency?
Legal certainty?

↓

NO TRUST


GDPR
requirements
controller
processor
organisational
technical
Risk based approach
Encryption
WITDOM
Trust in traditionally untrusted

Partners







Contact

griet.verhenneman@kuleuven.be
witdom.eu

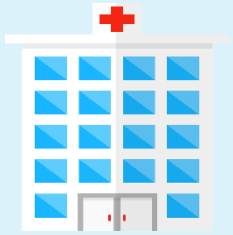

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 64437. This work was supported in part by the Swiss State Secretariat for Education, Research and Innovation under contract No. 15.0098. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission or the Swiss Government.

How to create trust in the untrusted?

- Availability and confidentiality
- Data isolation for purpose limitation
- Cryptography in transit and at rest
- GDPR compliance

GDPR requirements when outsourcing

- Outsourcing does not alter the set of measures to comply with. The same organisational and technical measures have to be implemented.
- Outsourcing alters the consequences of these measures:

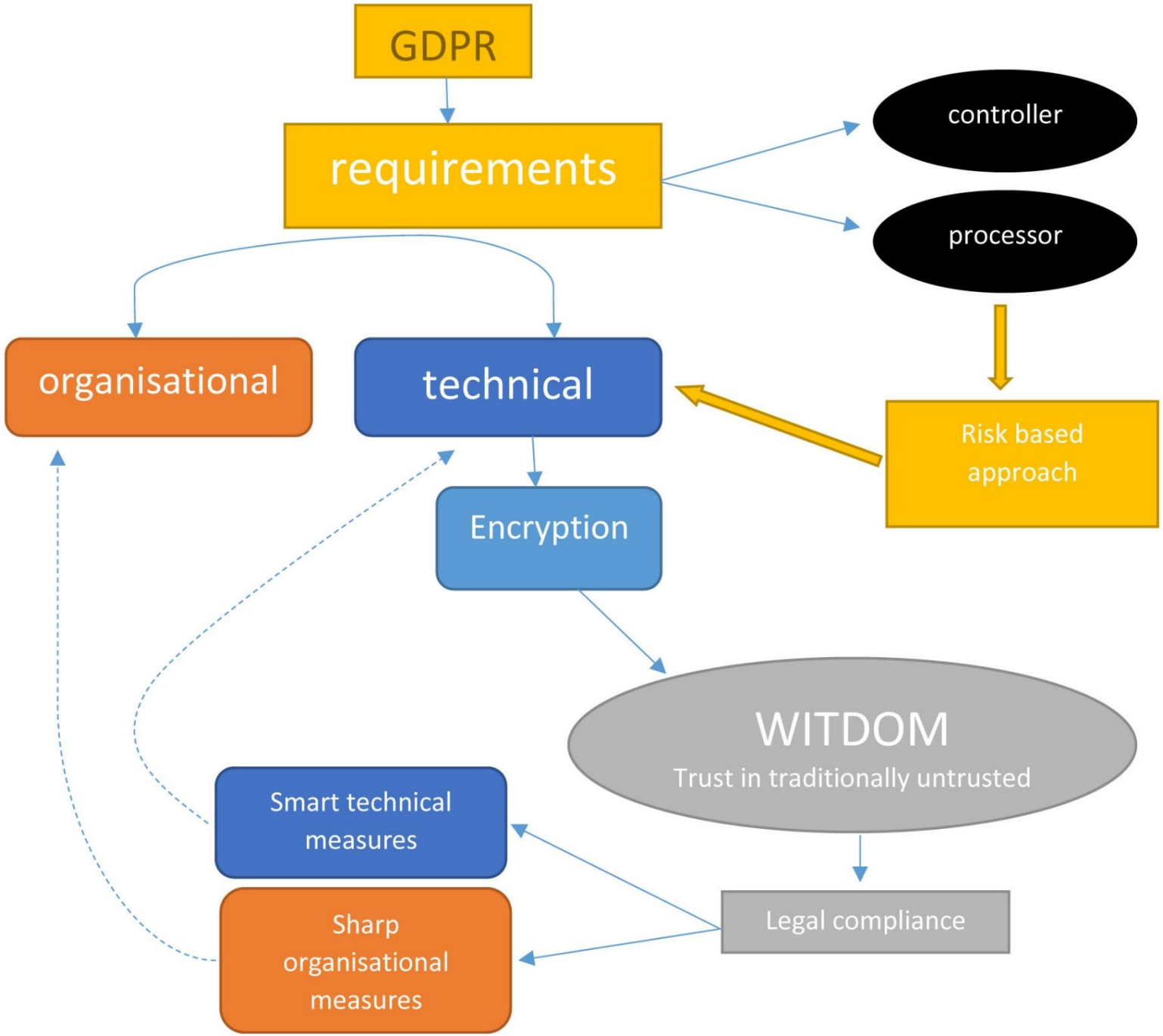


Client

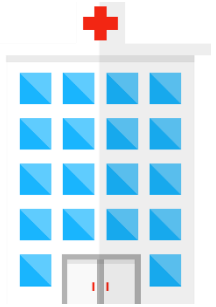
Responsible for
- Choice of service provider
- Organisational measures

Service provider

Responsible for
- Security of the service
- Technical guarantees will sell the service

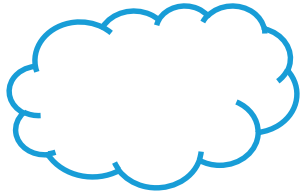

GDPR
requirements
controller
processor
organisational
technical
Risk based approach
Encryption
WITDOM
Trust in traditionally untrusted
Smart technical measures
Sharp organisational measures
Legal compliance

1



Internal pre-processing analysis

2



Internal pre-outsourcing analysis

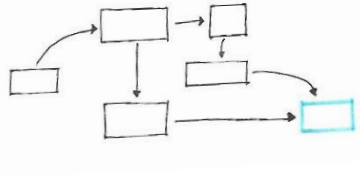
3

B2B contract

4

Informed Consent process where neede

5



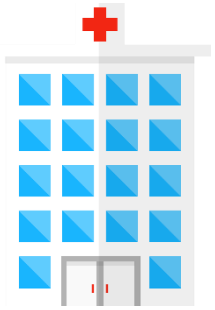
Internal procedures

6

Alert raising events

KU LEUVEN
CENTRE FOR IT & IP LAW

1. Internal pre-processing analysis

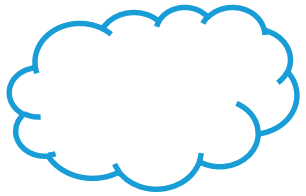


Ensure the legality and legitimacy of the data processing through an internal pre-processing analysis (whether or not as part of obligation for DPIA)

For example:

- What is the purpose of the data processing?
- Am I compliant with the need-to-know requirement? Data minisation.
- Are the processed data accurate and how will we keep them accurate?
- Is an approval required for the data processing? By sectoral committee? By ethics committee? By any other authority?
- Are information policies developed to inform the data subject?

2. Internal pre-outsourcing analysis



Ensure the legitimacy and legality of the data transfer to the third party service

For example:

- Does the outsourcing compromise the purpose of the data processing?
- How are the data flows affected? Is the register updated accordingly?
- In case the outsourcing involves a partner in a third country, is the data subject informed?

3. B2B contract

GDPR strengthens the contractual relationship between controller and processor.

- ↑ minimum clauses in controller-processor agreement
- ↑ liabilities for processor

Note: GDPR only considers actual relationship between parties, does not really care about contractual divergence.

For example

- Is confidentiality ensured contractually: contractual or professional secrecy?
- Does the third party guarantee to not further process the transferred data?
- Does the third party provide you with a DPIA?

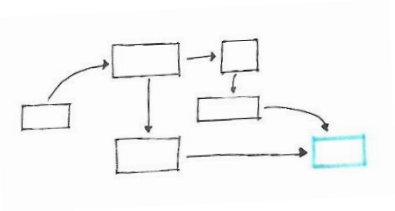
4. Informed consent process (if needed)

Informed consent has become stricter in GDPR and therefore devaluates as legal ground. If needed, however: comply with all requirements.

For example:

- Is the informed consent given freely considering all circumstances and the context?
- Is the informed consent explicit?
- Do you have a documented informed consent procedure?
- Does the informed consent explain the rights of the individual?
- Can informed consent be withdrawn?

5. Internal procedures



Certain internal procedures need to be in place in order to ensure compliance not only at start of the data processing, but during the complete life cycle.

For example:

- Are procedures in place for the removal of personal data after expiration of the retention period?
- Is the third party able to adequately respond to a request to delete personal data?
- Does the system perform a check on the availability and validity of the informed consent?
- Are procedures in place to respond to requests from the data subject? (access, removal, withdrawal consent,…)

Tools for GDPR automation

At company side:

- Master data management (MDM) solutions and GDPR sniffers (data lake)
- Data catalogue / data store solutions (amazonification of data)
- Incident response management systems and request management systems
- Risk and compliance management systems
- Consent management systems

At consumer side:

- Automated access requests

6. Define alert raising events

It could be well worth to include automated alerts for certain events which require an organisational action.

- Death of data subject
- Expiration of retention period
- Expiration of security assessment

Conclusions

1. GDPR is build on and soaked with **“risk based approach”**.

2. GDPR is **technology agnostic**: the technological state of the art determines which security measures should be implemented

3. GDPR considers **encryption a basic safeguard** and one of the means to create trust.

4. Controllers and processors will be held **liable for not choosing the appropriate security measures**, including encryption, and risk:
    1. Data breach notifications & trial by media
    2. Administrative fines imposed by DPA
    3. Penal sanctions in case of court-case

5. Compliance can only be achieved through combination of **smart technical and sharp organisational measures**.

KU Leuven Centre for IT & IP Law - iMinds
Sint-Michielsstraat 6, box 3443
BE-3000 Leuven, Belgium

http://www.law.kuleuven.be/citip
griet.verhenneman@kuleuven.be

KU LEUVEN
CENTRE FOR IT & IP LAW